REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

Claims 1, 3-7 and 9-13 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter. While not acquiescing in this rejection, method claim 7 has been amended to require storing the determination of whether the file can be regarded as safe. Consequently, Applicant respectfully submits that claim 7 and its dependent claims 9-12 are directed to statutory subject matter. With respect to independent claims 1 and 13 and the claims that depend therefrom, these are system claims comprising structural elements and are clearly directed to statutory subject matter. Indeed, the MPEP excerpt on which the Section 101 rejection is predicated (i.e., MPEP 2106 IV.B.2(b)) is expressly directed to process claims and does not constitute a basis for rejecting the pending system claims. Consequently, reconsideration of the Section 101 rejection with respect to these system claims is respectfully submitted.

Claims 1, 3-7 and 9-13 were rejected under 35 U.S.C. Section 102(b) as allegedly being "anticipated" by Roberts et al. (US-2004/0088570). Reconsideration of this rejection is respectfully requested.

First, Roberts et al. was not published more than one year before the effective filing date of the subject patent application and thus the rejection is not properly made under Section 102(b).

Second, Applicant respectfully submits that at least feature of (c) of claim 1 is not disclosed by Roberts et al. Feature (c) reads:

> c) means for determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected and for controlling the means b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the means b) at all.

The office action alleges that the feature (c) is disclosed in paragraph 37, lines 8-18 of Roberts et al. Applicant respectfully submits that this is incorrect for at least the following reasons.

Roberts et al. discloses a system implemented in a firewall in which webpages identified by links in documents (e.g. emails or files) are scanned for malware pre-emptively. Thus when the user subsequently clicks on the link, the webpage can be retrieved without scanning it again. This avoids a delay associated with scanning the webpage after the user clicks on the link.

Paragraph 34, lines 6-8 of Roberts et al. discloses that, in the database of addresses which have been preemptively scanned and found safe, there is stored various page version identifying data including a date which is presumably therefore the date of creation of that version of the webpage.

Paragraph 37, lines 8-16 of Roberts et al. discloses a first way of performing the check in the step 50 of whether the webpage has changed since it was scanned. This is to compare a checksum stored in the database with a checksum for the new webpage. Clearly this first way of performing the check in step 50 of Roberts et al. does not anticipate feature (c) of claim 1, because it does not involve consideration of the factor of "the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected".

Paragraph 37, lines 16-18 of Roberts et al. discloses a first way of performing the check in step 50 of whether the webpage has changed since it was scanned. This sentence reads:

> Another mechanism may use dates or other information embedded within the webpage being accessed to determine its currency or status.

Again this second way of way performing the check in step 50 of Roberts et al. does not anticipate feature (c) of claim 1, because it does not involve consideration of the factor of "the length of time for which the database indicates that the file has been known without maleware-containing instances of it being detected".

Although the above-referenced sentence in Roberts et al. refers to "dates or other information embedded in the webpage" this does not mean that Roberts et al. is referring to "the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected". To the contrary, the sentence must be read in context

as describing one way of performing the check in step 50 of whether the webpage has changed since it was scanned.

In that context, the skilled person reading Roberts et al. would understand the sentence to describe using dates or other information embedded in the webpage to determine whether the webpage has changed since it was scanned. The would perhaps best be understood as describing a comparison of a "Date Modified" field in the metadata of the webpage with the date recorded in the database when the webpage was preemptively scanned (as disclosed in paragraph 34, line 7). In that case, clearly the date being checked does not give any information about "the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected".

Even if some other meaning is ascribed to this text, in the context that the sentence describes a way of determining whether the webpage has changed since it was scanned, clearly Roberts et al. is not describing "the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected", because there is no disclosure that the "date" to which Roberts et al. refers has any relationship to whether a malware-containing instance of the webpage has been detected in any period.

This point is in line with the entire thrust of the teaching of Roberts et al. that a webpage does not need scanning again if it has not changed since it was preemptively scanned. Thus the purpose of step 50 on which the office action relies is to determine that the webpage has changed since it was preemptively scanned.

It follows that Roberts et al. does not disclose that "the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected" as recited in feature (c) of claim 1 can be used as a basis for determining that the file is regarded to be safe and hence can be subject to less thorough processing. As this feature is explicitly recited in claim 1, Roberts et al. cannot anticipate claim 1.

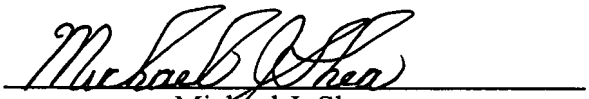
The other independent claims 7 and 13 contain similar recitations and are therefore not anticipated by Roberts et al. for similar reasons.

The rejection of dependent claims 3-6 and 9-12 is respectfully traversed at least because of their dependencies on independent claims 1 and 7.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Michael J. Shea
Reg. No. 34,725

MJS:dbp
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100